

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
FREDERICK D. WEBER
DALE E. GULICK
GEOFFREY S. STRONGIN

Serial No.: 09/870,889

Filed: 05/30/2001

For: EXTERNAL LOCKING MECHANISM
FOR PERSONAL COMPUTER MEMORY

Examiner: M. Chery

Group Art Unit: 2188

Att'y Docket: 2000.038800

Customer No. 023720

APPEAL BRIEF

Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING 37 C.F.R. 1.8	
I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date below:	
<u>02-21-06</u> Date	<u>Kathy Jones</u> Signature

Sir:

Applicants hereby submit this Appeal Brief to the Board of Patent Appeals and Interferences in response to the final Office Action dated October 21, 2005. A Notice of Appeal was filed on January 10, 2006 and so this Appeal Brief is believed to be timely filed.

The Commissioner is authorized to deduct the fee for filing this Appeal Brief (\$500) from **Advanced Micro Devices, Inc.'s Deposit Account 01-0365/TT3761.¹**

02/28/2006 MAHME1 00000026 010365 09870889

01 FC:1401 500.00 DA

¹ In the event the monies in that account are insufficient, the Director is authorized to withdraw funds from Williams, Morgan & Amerson, P.C. Deposit Account No. 50-0786/2000.038800.

I. REAL PARTY IN INTEREST

The present application is owned by Advanced Micro Devices, Inc. The assignment of the present application to Advanced Micro Devices, Inc., is recorded at Reel 11882, Frame 0873.

II. RELATED APPEALS AND INTERFERENCES

Applicants are not aware of any related appeals and/or interferences that might affect the outcome of this proceeding.

III. STATUS OF THE CLAIMS

Claims 1-9, 21-24, 35-38, and 49-52 are pending in the present application. Claims 1, 3, 6, 21-24, 35-38, and 49-52 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Hotley (U.S. Patent No. 5,442,704) in view of Gephardt, et al (U.S. Patent No. 5,623,673). Claims 4, 7-8, and 26-27 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hotley and Gephardt in view of Gafken (U.S. Patent No. 6,026,016). Claims 2, 5, and 28 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hotley and Gephardt in view of Watts (U.S. Patent No. 6,816,925).

IV. STATUS OF AMENDMENTS

There were no amendments after the final rejections.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claims 1, 21, 35, and 49 set forth, among other things, determining whether the computer system is operating in a system management mode (SMM) and one or more locks

configured to control access to one or more of the plurality of memory units based on the determination of whether the computer system is operating in the system management mode (SMM). For example, the embodiment of the SMM access controller 402 illustrated in Fig. 6 includes the one or more access locks 460 within the SMM access filters 410. The access locks 460 provide a means of preventing (or locking) and allowing (or unlocking) access to one or more of the devices within the security hardware 370C. See Patent Application, page 25, ll. 23-25. The access locks 460 may be opened in response to an SMI# or in response to the processor 102 or 805 entering SMM. See Patent Application, page 26, ll. 10-11.

Independent claim 35, in particular, sets forth a computer system that includes means for requesting a memory transaction for one or more memory addresses, means for determining a lock status for the one or more memory addresses, means for returning the lock status for the one or more memory addresses, and means for determining whether the computer system is operating in a system management mode (SMM). Independent claim 35 also sets forth means for determining, based on the determination of whether the computer system is operating in the system management mode (SMM), if the lock status for the one or more memory addresses can be changed if the lock status indicates that the memory transaction for the one or more memory addresses is not allowed and means for changing the lock status of the one or more memory addresses to allow the memory transaction if the lock status of the one or more memory addresses can be changed.

For example, in one embodiment, in response to receiving a request to enter the HDT mode (step 3305), an HDT control logic 3110 checks the status of the one or more HDT enable lock bits to determine if the HDT lock mode is locked or unlocked (step 3310). If the HDT lock mode is unlocked (step 3315), then the HDT control logic 3110 initiates HDT mode (step 3335).

If the HDT lock mode is locked (step 3315), then the HDT control logic 3110 requests authorization to change the HDT lock mode status (step 3320). If the change is authorized (step 3325), then the HDT control logic 3110 changes the HDT mode lock bit to unlocked (step 3330). If the change is not authorized (step 3325), then the HDT control logic 3110 does not change the HDT mode lock bit. In various embodiments, the HDT enable status may be changed by setting or resetting the one or more HDT enable status bits. For example, the HDT mode may be disabled, but inside SMM, a predetermined input to the HDT control logic 3110 may signal the HDT control logic 3110 to change the HDT mode status to enabled. In the embodiment of Fig. 20A, for example, once signaled, the HDT control logic 3110 would change the status of the HDT enable bit from disabled to enabled.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellant respectfully requests that the Board review and overturn the three rejections present in this case. The following issues are presented on appeal in this case:

- (A) Whether claims 1, 3, 6, 21-24, 35-38, and 49-52 are obvious over Hotley in view of Gephardt, et al;
- (B) Whether claims 4, 7-8, and 26-27 are obvious over Hotley and Gephardt in view of Gafken; and
- (C) Whether claims 2, 5, and 28 are obvious over Hotley and Gephardt in view of Watts.

VII. ARGUMENT

A. Legal Standards

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974). Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. That is, there must be something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561 (Fed. Cir. 1986). In fact, the absence of a suggestion to combine is dispositive in an obviousness determination. *Gambro Lundia AB v. Baxter Healthcare Corp.*, 110 F.3d 1573 (Fed. Cir. 1997). The mere fact that the prior art can be combined or modified does not make the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990); M.P.E.P. § 2143.01. Third, there must be a reasonable expectation of success.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991); M.P.E.P. § 2142. A recent Federal Circuit case emphasizes that, in an obviousness situation, the prior art must disclose each and every element of the claimed invention, and that any motivation to combine or modify the prior art must be based upon a suggestion in the prior art. *In re Lee*, 61 U.S.P.Q.2d 143 (Fed. Cir. 2002). Conclusory statements regarding common knowledge and common sense are insufficient to support a finding of obviousness. *Id.* at 1434-35. Moreover, it is the claimed

invention, as a whole, that must be considered for purposes of determining obviousness. A mere selection of various bits and pieces of the claimed invention from various sources of prior art does not render a claimed invention obvious, unless there is a suggestion or motivation in the prior art for the claimed invention, when considered as a whole.

B. Claims 1, 3, 6, 21-24, 35-38, and 49-52 are not obvious over Hotley in view of Gephardt.

Hotley describes a secure memory card that includes a security access control unit and a chip memory. The chip memory is organized into a number blocks having a number of rows, and each row includes a single lock bit location that may provide storage for lock bits within each block. The security access control unit may perform a predetermined key validation operation for a protected block by serially comparing bits of the key value against the bit contents of the lock bit positions of the memory block. See Hotley, col. 3, ll. 4-27. However, as admitted by the Examiner, Hotley is completely silent with regard to a system management mode (SMM). As stated in the specification of the present application, System Management Mode (SMM) is a mode of operation in the computer system that was implemented to conserve power. The SMM was created for the fourth generation x86 processors. See Patent Application, page 15, ll. 13-17.

The Examiner relies upon Gephardt to describe a system management mode for use in a computing system 200. Gephardt describes a lock-out register 216 that may be used for locking a system management space 410 used to store system management routines. After the system management routines are loaded into the system management space 410, the lock-out register 216 is set such that the system management routines cannot be overwritten during a normal

mode of operation. Once the lock-out register 216 is set by system software it cannot be subsequently reset while the system is in the normal mode. The system management space 410 can be accessed while operating in the system management mode or the debug system management mode regardless of the state of the lock-out register. See Gephardt, col. 9, ll. 1-27.

The Examiner then alleges that a person of ordinary skill in the art would be motivated to implement the lock-out registers 216 described by Gephardt in the smart card described by Hotley to restrict access to system management routines. Applicants respectfully disagree for at least the following reasons. First, Applicants respectfully submit that the cited references provide no suggestion or motivation for implementing a system management mode on a smart card. In particular, the cited references provide no indication that smart cards require any of the power management functions that may be provided in the system management mode. Second, Applicants respectfully submit that a person of ordinary skill in the art would not use the memory rows described by Hotley to store system management routines or any other routine. In particular, routines are not generally stored in a row-by-row structure and therefore protecting individual rows using a lock bit (as described by Hotley) would inhibit operation of these routines. Third, Applicants respectfully submit that a person of ordinary skill in the art would not implement the lock-out registers 216 described by Gephardt on the smart card described by Hotley at least in part because the lock-out registers 216 completely block access to the protected memory during a normal mode of operation, whereas the smart card described by Hotley is designed to allow access to protected registers following an authentication procedure.

Thus, Applicants respectfully submit that the Examiner has merely selected various bits and pieces of the claimed invention from various sources of prior art. However, as discussed above, the cited references provide no suggestion or motivation to combine and/or modify the

prior art of record to arrive at the claimed invention. Furthermore, Applicants respectfully submit that the cited references provide no reasonable expectation of success. In particular, Applicants respectfully submit that the cited references provide no reasonable expectation that simply combining elements of Hotley and Gephardt in the manner suggested by the Examiner would result in a computer system that could determine whether the computer system is operating in a system management mode (SMM) and includes one or more locks configured to control access to one or more of the plurality of memory units based on the determination of whether the computer system is operating in the system management mode (SMM).

For at least the aforementioned reasons Applicants respectfully submit that the Examiner has failed to make a *prima facie* case that the present invention is obvious over the cited references. Applicants respectfully request that the Examiner's rejections of claims 1, 3, 6, 21-24, 35-38, and 49-52 under 35 U.S.C. § 103(a) be REVERSED.

C. Claims 4, 7-8, and 26-27 are not obvious over Hotley and Gephardt in view of Gafken.

As discussed above, Applicants respectfully submit that the Examiner has merely selected various bits and pieces of the claimed invention from Hotley and Gephardt in an attempt to reproduce the claimed invention. However, as discussed above, the cited references provide no suggestion or motivation to combine and/or modify the prior art of record to arrive at the claimed invention. Furthermore, Applicants respectfully submit that the cited references provide no reasonable expectation of success.

In rejecting claims 4, 7-8, and 26-27, the Examiner relies on Gafken to describe a read lock bit, a write lock bit, and a lockdown bit. However, Gafken fails to remedy the fundamental deficiencies of the primary references.

For at least the aforementioned reasons, Applicants respectfully submit that the Examiner has failed to make a *prima facie* case that the present invention is obvious over the cited references. Applicants respectfully request that the Examiner's rejections of claims 4, 7-8, and 26-27 under 35 U.S.C. § 103(a) be REVERSED.

D. Claims 2, 5, and 28 are not obvious over Hotley and Gephardt in view of Watts.

As discussed above, Applicants respectfully submit that the Examiner has merely selected various bits and pieces of the claimed invention from Hotley and Gephardt in an attempt to reproduce the claimed invention. However, as discussed above, the cited references provide no suggestion or motivation to combine and/or modify the prior art of record to arrive at the claimed invention. Furthermore, Applicants respectfully submit that the cited references provide no reasonable expectation of success.

In rejecting claims 4, 7-8, and 26-27, the Examiner relies on Watts to describe a low pin count (LPC) bus protocol. However, Watts fails to remedy the fundamental deficiencies of the primary references.

For at least the aforementioned reasons, Applicants respectfully submit that the Examiner has failed to make a *prima facie* case that the present invention is obvious over the cited references. Applicants respectfully request that the Examiner's rejections of claims 2, 5, and 28 under 35 U.S.C. § 103(a) be REVERSED.

VIII. CLAIMS APPENDIX

The claims that are the subject of the present appeal – claims 1-9, 21-24, 35-38, and 49-52 – are set forth in the attached “Claims Appendix.”

IX. EVIDENCE APPENDIX

There is no separate Evidence Appendix for this appeal.

X. RELATED PROCEEDINGS APPENDIX

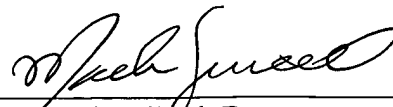
There is no Related Proceedings Appendix for this appeal.

XI. CONCLUSION

In view of the foregoing, it is respectfully submitted that the Examiner erred in not allowing all claims pending in the present application, claims 1-9, 21-24, 35-38, and 49-52, over the prior art of record. The undersigned may be contacted at (713) 934-4052 with respect to any questions, comments or suggestions relating to this appeal.

Respectfully submitted,

Date: 2/21/06



Mark W. Sincell, Ph.D.
Reg. No. 52,226
WILLIAMS, MORGAN & AMERSON
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-7000
(713) 934-7011 (facsimile)

AGENT FOR APPLICANTS

CLAIMS APPENDIX

1. (Previously Presented) A computer system, comprising:

a bus;

a memory coupled to the bus, wherein the memory includes a plurality of storage locations,

wherein the plurality of storage locations are divided into a plurality of memory units;

and

a device coupled to access the memory over the bus, the device being configured to determine

whether the computer system is operating in a system management mode (SMM), and

wherein the device includes one or more locks configured to control access to one or

more of the plurality of memory units based on the determination of whether the

computer system is operating in the system management mode (SMM).
2. (Previously Presented) The computer system of claim 1, wherein the bus is configured to

operate according to a low pin count (LPC) bus protocol.
3. (Original) The computer system of claim 1, wherein the memory is a ROM.
4. (Original) The computer system of claim 3, wherein the ROM is a BIOS ROM.
5. (Original) The computer system of claim 1, wherein the device is a south bridge.

6. (Original) The computer system of claim 1, wherein the locks include a plurality of registers, wherein one or more entries in one or more of the plurality of registers indicate an access control setting for one or more of the memory units.
7. (Original) The computer system of claim 6, wherein at least one of the plurality of registers is configured to store three locking bits for one of the memory blocks, wherein the three locking bits include a read lock bit, a write lock bit, and a lock-down bit, wherein the read lock bit and the write lock bit are permanent until reset when the lock-down bit is set.
8. (Original) The computer system of claim 6, wherein at least one of the plurality of registers is configured to store eight bits, wherein the eight bits include three locking bits for one of the memory blocks and another three locking bits for another one of the memory blocks, wherein the three locking bits include a first read lock bit, a first write lock bit, and a first lock-down bit, wherein when the first lock-down bit is set, the first read lock bit and the first write lock bit are permanent until reset, and wherein the another three locking bits include a second read lock bit, a second write lock bit, and a second lock-down bit, wherein when the second lock-down bit is set, the second read lock bit and the second write lock bit are permanent until reset.
9. (Previously Presented) The computer system of claim 8, wherein the at least one of the plurality of registers is configured with bit 0 as the first write lock bit, bit 1 as the first lock-down bit, bit 2 as the first read lock bit, bit 4 as the second write lock bit, bit 5 as the second lock-down bit, and bit 6 as the second read lock bit.

10. (Withdrawn) A memory, comprising:
 - a first plurality of storage locations configured with BIOS data; and
 - a second plurality of storage locations, wherein the second plurality of storage locations includes:
 - a first plurality of blocks readable only in SMM; and
 - a second plurality of blocks readable in SMM and at least one operating mode other than SMM.
11. (Withdrawn) The memory of claim 10, wherein the at least one counter comprises a monotonic counter.
12. (Withdrawn) The memory of claim 10, wherein the second plurality of storage locations further includes:
 - at least one counter stored in a flat memory space.
13. (Withdrawn) The memory of claim 12, wherein the first plurality of blocks includes a block with a write once lock.
14. (Withdrawn) The memory of claim 12, wherein the first plurality of blocks includes a block with a never erase lock.
15. (Withdrawn) The memory of claim 12, wherein the first plurality of blocks includes a block that can be written in SMM and in at least one operating mode other than SMM.

16. (Withdrawn) The memory of claim 12, wherein the second plurality of blocks includes a block with a write once lock.
17. (Withdrawn) The memory of claim 12, wherein the second plurality of blocks includes a block with a never erase lock.
18. (Withdrawn) The memory of claim 12, wherein the plurality of blocks includes a block that can be written in SMM and in at least one operating mode other than SMM.
19. (Withdrawn) The memory of claim 10, wherein the first plurality of storage locations are addressed in an address range including from FFFF,FFFFh to FFC0,0000h.
20. (Withdrawn) The memory of claim 10, wherein the second plurality of storage locations are addressed in an address range including from FFBF,FFFFh to FFB0,0000h
21. (Previously Presented) A method for operating a computer system, the method comprising:
 - requesting a memory transaction for one or more memory addresses;
 - determining a lock status for the one or more memory addresses;
 - returning the lock status for the one or more memory addresses;
 - determining whether the computer system is operating in a system management mode (SMM);

determining, based on the determination of whether the computer system is operating in the system management mode(SMM), if the lock status for the one or more memory addresses can be changed if the lock status indicates that the memory transaction for the one or more memory addresses is not allowed;

changing the lock status of the one or more memory addresses to allow the memory transaction if the lock status of the one or more memory addresses can be changed.

22. (Original) The method of claim 21, wherein determining a lock status includes reading a first lock bit; and wherein returning the lock status includes returning the value of the first lock bit.

23. (Original) The method of claim 22, wherein determining if the lock status for the one or more memory address can be changed includes reading a second lock bit.

24. (Original) The method of claim 23, wherein changing the lock status of the one or more memory addresses to allow the memory transaction includes changing the value of the first lock bit.

25. (Withdrawn) A method of operating a computer system, the method comprising:
issuing a request from a first device for a memory transaction for a memory location;
receiving the request for the memory transaction at a second device that does not include the memory location or a copy of the contents of the memory location;

returning a response from the second device to the first device issuing the request for the memory transaction.

26. (Withdrawn) The method of claim 25, wherein returning the response from the second device includes ending the memory transaction without the memory transaction reaching the memory location.

27. (Withdrawn) The method of claim 25, further comprising:
ending the request for the memory transaction without the memory location responding to the request for the memory transaction.

28. (Withdrawn) The method of claim 25, wherein the second device includes a bridge coupled between the first device and the memory location, wherein said returning the response from the second device to the first device issuing the request for the memory transaction includes returning the response from the bridge to the first device issuing the request for the memory transaction.

29. (Withdrawn) The method of claim 28, wherein said returning the response from the bridge to the first device issuing the request for the memory transaction includes responding from an access filter within the bridge with a predetermined value upon receipt of the request for the memory transaction for the memory location, when the computer system is operating in a first operating mode.

30. (Withdrawn) The method of claim 29, wherein said issuing the request from the first device for the memory transaction for the memory location includes issuing the request from the first device for the memory transaction for the memory location in a ROM.
31. (Withdrawn) The method of claim 29, wherein said issuing the request from the first device for the memory transaction for the memory location includes issuing the request from the first device for the memory transaction for the memory location in a flash memory.
32. (Withdrawn) The method of claim 25, wherein said issuing the request from the first device for the memory transaction for the memory location includes issuing the request from the first device for the memory transaction for the memory location in a memory.
33. (Withdrawn) The method of claim 25, wherein the first device includes security hardware, wherein said receiving the request for the memory transaction at the second device that does not include the memory location or the copy of the contents of the memory location includes receiving the request for the memory transaction at the security hardware within the first device; and wherein said returning the response from the second device to the first device issuing the request for the memory transaction includes returning the response from the security hardware to the first device issuing the request for the memory transaction.

34. (Withdrawn) The method of claim 25, further comprising:

reading a first value from a memory location within the second device before returning the response, wherein the memory location within the second device is different from the memory location for the memory transaction.

35. (Previously Presented) A computer system, comprising:

means for requesting a memory transaction for one or more memory addresses;

means for determining a lock status for the one or more memory addresses;

means for returning the lock status for the one or more memory addresses;

means for determining whether the computer system is operating in a system management mode (SMM);

means for determining, based on the determination of whether the computer system is operating in the system management mode (SMM), if the lock status for the one or more memory addresses can be changed if the lock status indicates that the memory transaction for the one or more memory addresses is not allowed;

means for changing the lock status of the one or more memory addresses to allow the memory transaction if the lock status of the one or more memory addresses can be changed.

36. (Original) The computer system of claim 35, wherein the means for determining the lock status comprises means for reading a first lock bit; and wherein the means for returning the lock status includes means for returning the value of the first lock bit.

37. (Original) The computer system of claim 36, wherein determining if the lock status for the one or more memory address can be changed includes reading a second lock bit.
38. (Original) The computer system of claim 37, wherein the means for changing the lock status of the one or more memory addresses to allow the memory transaction includes means for changing the value of the first lock bit.
39. (Withdrawn) A computer system, comprising:
means for issuing a request from a first device for a memory transaction for a memory location;
means for receiving the request for the memory transaction at a second device that does not include the memory location or a copy of the contents of the memory location; and
means for returning a response from the second device to the first device issuing the request for the memory transaction.
40. (Withdrawn) The computer system of claim 39, wherein the means for returning the response from the second device includes means for ending the memory transaction without the memory transaction reaching the memory location.
41. (Withdrawn) The computer system of claim 39, further comprising:
means for ending the request for the memory transaction without the memory location responding to the request for the memory transaction.

42. (Withdrawn) The computer system of claim 39, wherein the second device includes a bridge coupled between the first device and the memory location, wherein the means for returning the response from the second device to the first device issuing the request for the memory transaction includes means for returning the response from the bridge to the first device issuing the request for the memory transaction.
43. (Withdrawn) The computer system of claim 42, wherein the means for returning the response from the bridge to the first device issuing the request for the memory transaction includes means for responding from an access filter within the bridge with a predetermined value upon receipt of the request for the memory transaction for the memory location, when the computer system is operating in a first operating mode.
44. (Withdrawn) The computer system of claim 43, wherein the means for issuing the request from the first device for the memory transaction for the memory location includes means for issuing the request from the first device for the memory transaction for the memory location in a ROM.
45. (Withdrawn) The computer system of claim 43, wherein the means for issuing the request from the first device for the memory transaction for the memory location includes means for issuing the request from the first device for the memory transaction for the memory location in a flash memory.

46. (Withdrawn) The computer system of claim 39, wherein the means for issuing the request from the first device for the memory transaction for the memory location includes means for issuing the request from the first device for the memory transaction for the memory location in a memory.
47. (Withdrawn) The computer system of claim 39, wherein the first device includes security hardware, wherein the means for receiving the request for the memory transaction at the second device that does not include the memory location or the copy of the contents of the memory location includes means for receiving the request for the memory transaction at the security hardware within the first device; and wherein the means for returning the response from the second device to the first device issuing the request for the memory transaction includes means for returning the response from the security hardware to the first device issuing the request for the memory transaction.
48. (Withdrawn) The computer system of claim 39, further comprising:
means for reading a first value from a memory location within the second device before returning the response, wherein the memory location within the second device is different from the memory location for the memory transaction.
49. (Previously Presented) A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of operating the computer system, the method comprising:
requesting a memory transaction for one or more memory addresses;

determining a lock status for the one or more memory addresses;
returning the lock status for the one or more memory addresses;
determining whether the computer system is operating in a system management mode (SMM);
determining, based on the determination of whether the computer system is operating in the system management mode (SMM), if the lock status for the one or more memory addresses can be changed if the lock status indicates that the memory transaction for the one or more memory addresses is not allowed;
changing the lock status of the one or more memory addresses to allow the memory transaction if the lock status of the one or more memory addresses can be changed.

50. (Original) The computer readable program storage device of claim 49, wherein determining a lock status includes reading a first lock bit; and wherein returning the lock status includes returning the value of the first lock bit.

51. (Original) The computer readable program storage device of claim 50, wherein determining if the lock status for the one or more memory address can be changed includes reading a second lock bit.

52. (Original) The computer readable program storage device of claim 51, wherein changing the lock status of the one or more memory addresses to allow the memory transaction includes changing the value of the first lock bit.

53. (Withdrawn) A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of operating the computer system, the method comprising:

issuing a request from a first device for a memory transaction for a memory location;

receiving the request for the memory transaction at a second device that does not include the memory location or a copy of the contents of the memory location;

returning a response from the second device to the first device issuing the request for the memory transaction.

54. (Withdrawn) The computer readable program storage device of claim 53, wherein returning the response from the second device includes ending the memory transaction without the memory transaction reaching the memory location.

55. (Withdrawn) The computer readable program storage device of claim 53, the method further comprising:

ending the request for the memory transaction without the memory location responding to the request for the memory transaction.

56. (Withdrawn) The computer readable program storage device of claim 53, wherein the second device includes a bridge coupled between the first device and the memory location, wherein said returning the response from the second device to the first device issuing the request for the memory transaction includes returning the response from the bridge to the first device issuing the request for the memory transaction.

57. (Withdrawn) The computer readable program storage device of claim 56, wherein said returning the response from the bridge to the first device issuing the request for the memory transaction includes responding from an access filter within the bridge with a predetermined value upon receipt of the request for the memory transaction for the memory location, when the computer system is operating in a first operating mode.
58. (Withdrawn) The computer readable program storage device of claim 57, wherein said issuing the request from the first device for the memory transaction for the memory location includes issuing the request from the first device for the memory transaction for the memory location in a ROM.
59. (Withdrawn) The computer readable program storage device of claim 57, wherein said issuing the request from the first device for the memory transaction for the memory location includes issuing the request from the first device for the memory transaction for the memory location in a flash memory.
60. (Withdrawn) The computer readable program storage device of claim 53, wherein said issuing the request from the first device for the memory transaction for the memory location includes issuing the request from the first device for the memory transaction for the memory location in a memory.

61. (Withdrawn) The computer readable program storage device of claim 53, wherein the first device includes security hardware, wherein said receiving the request for the memory transaction at the second device that does not include the memory location or the copy of the contents of the memory location includes receiving the request for the memory transaction at the security hardware within the first device; and wherein said returning the response from the second device to the first device issuing the request for the memory transaction includes returning the response from the security hardware to the first device issuing the request for the memory transaction.
62. (Withdrawn) The computer readable program storage device of claim 53, the method further comprising:
reading a first value from a memory location within the second device before returning the response, wherein the memory location within the second device is different from the memory location for the memory transaction.